NUI Galway
OÉ Gaillimh

# ***Semester Two Examinations 2017/2018***

| | |
|---|---|
| **Exam Code(s)** | 4BCT1, 1MECE1, 1OA1, 1EM1 |
| **Exam(s)** | Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering, Overseas, Erasmus |
| **Module Code(s)** | CT437 |
| **Module(s)** | Computer Security and Forensic Computing |
| Paper No. | 1 |
| Repeat Paper | No |
| External Examiner(s) | Dr. Jacob Howe |
| Internal Examiner(s) | Prof M. Madden<br>*Dr. C. Mulvihill |

**Instructions:** Answer any 3 questions.
All questions will be marked equally.

| | |
|---|---|
| **Duration** | 2 hours |
| **No. of Pages** | 3 |
| **Discipline(s)** | Information Technology |
| **Course Co-ordinator(s)** | Dr. D. Chambers |

**Requirements**:

| | | | | |
|---|---|---|---|---|
| Release in Exam Venue | Yes | X | No | |
| MCQ | Yes | | No | X |
| Handout | None | | | |
| Statistical/ Log Tables | None | | | |
| Cambridge Tables | None | | | |
| Graph Paper | None | | | |
| Log Graph Paper | None | | | |
| Other Materials | None | | | |
| Graphic material in colour | Yes | | No | X |

**PTO**

1

(a) Entity authentication requires evidence of identity. This may be achieved via one, two, or three factors. Explain what is meant by each of the terms 'one factor', 'two factor' and 'three factor' authentication. (9 marks)

(b) Entity authentication also requires evidence of freshness. This can be provided by timestamps or, as one alternative, by so-called nonces. Give any one advantage and any one disadvantage of each such approach. (8 marks)

(c) Outline the steps involved in any one entity authentication scheme that is based on two-factor challenge-response between a user and a server. The scheme should make use of 'tokens' on which password functions have been implemented. (8 marks)

2

(a) The 'Daubert' criteria, in one instantiation, enumerate properties that should be possessed by a digital investigative technique in order to have confidence that evidence supplied by that technique is reliable. Outline any two of these criteria. (8 marks)

(b) Outline any two challenges that the so-called 'Internet of Things' may pose for digital forensics. (8 marks)

(c) 'Steganography presents a challenge for forensic investigators, not only from a technical perspective but also because of the possible defence of plausible deniability'. Outline why image-based steganography may be hard to find on a suspect device and explain what is meant by the term 'plausible deniability' in the course of your answer. (9 marks)

3

Consider the document 'Framework for Improving Critical Infrastructure Cybersecurity', released by the National Institute of Standards and Technology (NIST) in 2017. The framework presented in this document is, as stated in the document, a 'risk-based approach to managing cybersecurity risk'. Discuss this framework under the following three headings 'Framework Core' (9 marks), 'Framework Implementation Tiers' (8 marks), and 'Framework Profile' (8 marks).

4
(a) 'A cryptographic hash function should display preimage, second preimage and collision resistance'. Explain what is meant by each of the terms 'preimage resistance', 'second preimage resistance', and 'collision resistance'. (9 marks)

(b) Message Authentication Codes differ from a cryptographic hash function in that they employ a key. How does a key help (if it does) with data origin authentication? (8 marks)

(c) Consider an auction with sealed bids. Bids are protected by a cryptographic hash and it is this hash value that is submitted by a bidder. After the bidding process is completed the bidders reveal their bids, and these can then be checked against the submitted hashes. Suppose that the hash function employed in the auction fails to display collision resistance. Explain why the bidding process is vulnerable. (8 marks)

5
(a) By considering the sample plaintext '010101' and an associated keystream sample '011101', explain how encryption and decryption works for a stream cipher that depends on XOR. What problem would result with a keystream consisting of all zeroes for such a stream cipher? (8 marks)

(b) 'Block ciphers work on blocks rather than bits'. With the aid of a diagram, show one encryption round for either a generic Feistel cipher or the AES block cipher. (8 marks)

(c) 'A block cipher may be strengthened by introducing positional dependency'. Outline how encryption works for the block cipher mode of operation known as cipher block chain (CBC). Note: You do not have to consider decryption. (9 marks)

6
(a) In the context of public key infrastructure, explain what is meant by the terms 'certification authority', 'registration authority' and 'digital certificate'. (9 marks)

(b) An encryption scheme such as RSA depends in part on the assumed 'hardness' of certain problems which are believed to give rise to 'one-way' functions. Briefly outline any one such problem that RSA relies on, explaining the term 'one-way function' in the course of your answer. (8 marks)

(c) One approach to dealing with man-in-the middle attacks on Diffie-Hellman key exchange involves employing pre-existing signature/verification key pairs. Outline why such an approach might defeat man-in-the middle attacks. (8 marks)